REMARKS

[0011] Applicant respectfully requests reconsideration and allowance of all of the claims of the application. The status of the claims is as follows:

- Claims 1, 2, 4-9, 11, 17-31, 40-58 and 72-85 are currently pending;
- Claims 3, 10, 12-16, 32-39 and 59-71 are canceled;
- Claims 17-31, 40-55 and 72-85 are withdrawn;
- Claims 6, 9 and 58 are original;
- Claims 1, 2, 11, 56 and 57 are amended; and
- Claims 4, 5, 7, 8 and 57 are previously presented.

[0012] Independent claims 1, 56 and 57 are amended to include subject matter from a number of dependent claims.

Cited Documents

[0013] The following documents have been applied to reject one or more claims of the Application:

- Challener: U.S. Patent Application No. 2003/0105980;
- Bailey: U.S. Patent No. 7,205,883;
- Thomlinson: U.S. Patent No. 6,272,631; and
- Tewfik: U.S. Patent Application No. 2003/0095685.

Overview of the Application

[0014] The Application describes password-based key management, wherein a user can obtain encrypted data from a server by entering a user ID and a password. The

password is hashed and used to decrypt a user password to obtain a master password. Integrity checking and fraud prevention are disclosed.

Overview of Challener

[0015] Challenner describes a method for creating a password list for remote authentication. A data structure comprising paired user IDs and hashed passwords is disclosed.

Overview of Bailey

[0016] Bailey describes tamper detection and power failure recovery. An upper portion of column 6 discloses hashing a password to create a first key, and reversibly encrypting a second key with the first key.

Overview of Thomlinson

[0017] Thomlinson describes protected storage of core data secrets.

Overview of Tewfik

[0018] Tewflik describes detection of digital watermarking.

§ 103 Rejections

[0019] Claim 57 stands rejected under 35 U.S.C. § 103(a) as allegedly being obvious over Challener in view of Bailey. Applicant respectfully traverses the rejection.

Independent Claim 57

[0020] In light of the amendments presented herein, and the above-referenced discussion with the Examiner, Applicant submits that the rejection of independent claim 57 is moot.

[0021] Claim 57 recites:

57. A computer-readable medium having stored thereon computer executable instructions for performing acts of:

storing data encrypted with a master key;

creating a data structure comprising a plurality of user keys paired with user IDs, wherein each user key is associated with one of a plurality of users, respectively, and **wherein each of the plurality of user keys comprises a different encryption of the master key**, encrypted by operation of a reversible process using a hash value of a password associated with user, and **wherein each user key additionally comprises a keyed-hash message authentication code encrypted using the hash value of the password associated with the user**;

accessing, upon presentation of a user ID of a user, a user key associated with the user ID, from the data structure;

hashing, upon presentation of a password of the user, the presented password to produce a hash value;

preventing fraudulent access to data comprising: tracking attempts by a user to access data, and blocking attempts for a time period after a threshold number of failed attempts; reporting failed data access attempts to a system administrator according to user ID; increasing a time period a user must wait to attempt to access data after successive failed attempts to access the data; and, **deleting a user ID and a user key after a threshold number of failed attempts to access data**;

verifying the keyed-hash message authentication code encrypted using the hash of the password associated with the user;

decrypting the user key using the hash value, thereby creating the master key;

decrypting data using the master key; and

sending the data to the user.

[0022] Claim 57 has been amended to recite, in part:

- ***deleting a user ID and a user key after a threshold number of failed attempts to access data***

[0023] This element was previously recited by Claim 56, and is disclosed at least at the Applicant's specification at the bottom of page 18 and the top of page 19.

[0024] In rejecting Claim 56, with specific reference to the claimed, "deleting a user ID and a user key after a threshold number of failed attempts to access data" the Office suggested that Claim 56 was rejected for the same reason as Claim 1. However, Claim 1 did not recite, "deleting a user ID and a user key after a threshold number of failed attempts to access data". Moreover, the Applicant respectfully submits that the prior art of record does not teach or suggest such a "deleting". Accordingly, the Applicant submits that Claim 57, amended in a manner similar to Claim 56, recites subject matter not taught or suggested by the prior art of record, and respectfully submits that Claim 57 is in condition for allowance.

[0025] Claim 57 has also been amended to recite, in part:

- ***wherein each user key additionally comprises a keyed-hash message authentication code encrypted using the hash value of the password associated with the user***

[0026] This was previously recited in Claim 65, and as is disclosed at least at the Applicant's specification on page 14 and other locations.

[0027] In rejecting Claim 65, the Office suggested that Thomlinson at Fig. 3 and column 10 lines 30-57 teaches the MAC recited in Claim 65. The Applicant respectfully submits that Thomlinson teaches a MAC 133 that is generated from an Item Authentication Key 134 and a Data Item 130, and a MAC 142 that is generated from an Item Key 132 and a Master Authentication Key 143. The MAC 142 is of greater relevance, since it is related to the "key," while MAC 133 is related to the "item."

[0028] However, the Applicant respectfully submits that Thomlinson does not teach or suggest that either MAC is "*encrypted using the hash value of the password associated*

with the user". In particular, Thomlinson teaches that MAC 133 is encrypted using the key 134 and that the MAC 142 is encrypted using the key 143. The Applicant notes that the key 143 is encrypted at 145 using the user key 146 (which is a hash of the password 147). However, the MAC 142 is created with the unencrypted key 143, and not the encrypted result of 145 (all in Thomlinson's Fig. 3). That is, while Thomlinson teaches hashing a user's password, Thomlinson does not teach using the hash value to create the MAC. Thus, Thomlinson does not teach or suggest a MAC that is "*encrypted using the hash value of the password associated with the user*", as recited by Claim 57.

[0029] Accordingly, the Applicant submits that Claim 57, amended in a manner similar to Claim 65, recites subject matter not taught or suggested by the prior art of record, and respectfully submits that Claim 57 is in condition for allowance.

[0030] Claim 57 has also been amended to recite, in part:

- **wherein each of the plurality of user keys comprises a different encryption of the master key**

[0031] This is seen the Applicant's Fig. 2, wherein the table 126 comprises the various user IDs matched with user keys (UKi) that are formed from encryption of the master key using each user's hashed password.

[0032] In rejecting various claims, the Office pointed to Fig. 1 of the Challener reference, which teaches a table comprising paired user IDs and hashed passwords. Thus, Challener teaches encryptions of a plurality of different passwords in the table. In contrast, the claim recites, "wherein each of the plurality of user keys comprises a different encryption of the master key".

[0033] Thus, the Applicant submits that Thomlinson fails to teach or suggest a plurality of keys that are each a different encryption of the master key. Accordingly, the Applicant submits that Claim 57 recites subject matter not taught or suggested by the prior art of record, and respectfully submits that Claim 57 is in condition for allowance.

[0034] Dependent Claim 58 is allowable as a claim dependent on Claim 57, allowable for at least the reasons seen above. Additionally, Claim 58 is allowable for reasons associated with aspects recited in Claim 58.

Independent Claim 1

[0035] Claim 1 stands rejected under 35 U.S.C. § 103(a) as allegedly being obvious over Challener in view of Bailey, Thomlinson and Tewfik. Applicant respectfully traverses the rejection.

[0036] In light of the amendments presented herein, and the above-referenced discussion with the Examiner, the Applicant submits that the rejection of independent claim 1 is moot.

[0037] Claim 1 has been amended to recite:

- **deleting a user ID and a user key after a threshold number of failed attempts to access data**
- **the keyed-hash message authentication code, is based on the hash of the password and is added to each of the plurality of different encryptions of the master key**
- **a plurality of different encryptions of the master key such that the master key may be obtained by operation of any of a plurality of different keys, respectively**

[0038] In view of the amendments, the Applicant respectfully submits that Claim 1 is allowable for at least the reasons that Claim 57 is allowable, and the arguments and remarks from above are incorporated by reference at this location.

[0039] Dependent Claims 2, 4-9 and 11 are allowable as a claim dependent on Claim 1, allowable for at least the reasons seen above. Additionally, these claims are allowable for reasons associated with aspects recited in each.

Independent Claim 56

[0040] Claim 56 stands rejected under 35 U.S.C. § 103(a) as allegedly being obvious over Challener in view of Bailey, Thomlinson and Tewfik. Applicant respectfully traverses the rejection.

[0041] In light of the amendments presented herein, and the above-referenced discussion with the Examiner, the Applicant submits that the rejection of independent claim 56 is moot.

[0042] Claim 56 has also been amended to recite:

- **deleting a user ID and a user key after a threshold number of failed attempts to access data**
- **wherein each user key additionally comprises a keyed-hash message authentication code encrypted using the hash value of the password associated with the user**
- **wherein each of the plurality of user keys comprises a different encryption of the master key In view of the amendments**

[0043] The Applicant respectfully submits that Claim 56 is allowable for at least the reasons that Claim 57 is allowable, and the arguments and remarks from above are incorporated by reference at this location.

Conclusion

[0044] Applicant respectfully requests reconsideration and prompt issuance of the application. If any issues remain that prevent issuance of this application, the Examiner is urged to contact the undersigned representative for the Applicant before issuing a subsequent Action.

Respectfully Submitted,

Lee & Hayes, PLLC
Representative for Applicant

/David S. Thompson/ Dated: 23 March 2009

David S. Thompson

DavidT@LeeHayes.com
509-944-4735
Registration No. 37,954